CYBERMALVEILLANCE : COMMENT RECONNAÎTRE UN MESSAGE DE PHISHING ? AVEC CYBERMALVEILLANCE.GOUV.FR

Date de publication : **25/10/2021 - Internet/multimédia**

Maxime : "J’ai reçu un mail inhabituel de la part de ma banque. Comment savoir s’il s’agit d’un message sérieux ou d’une tentative de phishing ?".

C'est une bonne question Maxime. Le phishing est une technique de cyber malveillance utilisée par des fraudeurs pour vous voler des informations personnelles. Le tout, en empruntant l'identité d'un tiers de confiance, comme une administration, votre banque ou votre opérateur téléphonique. C'est pourquoi il est difficile d'identifier ce type de message frauduleux !

Il existe cependant des indices qui peuvent vous permettre de reconnaître un message de phishing. Quels sont-ils ?

Tout d'abord, un objet de message succinct ou alarmiste. Comme par exemple "remboursement", ou "alerte de sécurité". Le but est de vous inciter à ouvrir le message sans réfléchir.

Et un antivirus ne peut pas détecter ce genre de message frauduleux avant ouverture ?

Si. Votre antivirus peut vous signaler la réception d'un message malveillant. Prenez donc en compte cet avertissement. Par ailleurs, la réception d'un message inattendu, même d'apparence officielle, doit éveiller votre attention. Enfin, vous pouvez identifier un message d'hameçonnage, avant de l'ouvrir, si son expéditeur utilise une adresse d'expédition fantaisiste.

Le contenu du message peut également vous aider à repérer une tentative de phishing. Prenez garde aux discours aguicheurs ou inquiétants qui évoquent par exemple un gain d'argent, ou encore une action urgente à réaliser. De plus, ces messages peuvent parfois contenir des fautes d'orthographe ou de syntaxe, inhabituelles dans des communications officielles.

Redoublez de vigilance si le message comporte un lien ou une pièce jointe. Les fraudeurs souhaitent généralement vous pousser à ouvrir un document contenant un virus, ou vous faire cliquer sur un lien qui vous mènera sur un site frauduleux.

Enfin, au moindre doute, n'hésitez pas à contacter l'organisme dont semble provenir le message pour le lui faire confirmer et à vous renseigner sur le site de prévention et d'assistance Cybermalveillance.gouv.fr.

En résumé, ce qui doit vous alerter dans le mel :

- le fraudeur emprunte l'identité d'un tiers de confiance,
- l'objet du mel est succinct ou alarmiste,
- le mel est inattendu ou l'adresse fantaisiste,
- le mel concerne une promesse de gain d'argent ou un message d'urgence,
- le mel contient des fautes d'orthographe,
- vous avez une alerte de votre antivirus.
